UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/919,960	08/02/2001	Bruno Couillard	35997-215056	4262

26694 7590 09/12/2006

VENABLE LLP
P.O. BOX 34385
WASHINGTON, DC 20043-9998

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/919,960	**Applicant(s)** COUILLARD, BRUNO
	Examiner Michael Pyzocha	**Art Unit** 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 28 July 2006.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-31 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-31 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-31 are pending.

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 07/28/2006 has been entered.

Response to Amendment

3. The claim identifiers on many of the claims are incorrect stating a claim is previously presented when amendments were made to the claim. Also the claims with the (New) status identifier have underlined sections suggesting limitations were added to these claims when nothing was added. Appropriate changes are required in response to this action.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-9, 15-18, 28, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier (Applied Cryptography), in view of Ober et al (US 6307936), further in view of Arnold (US 6175924) and further in view of Fischer (US 6141423).

As per claims 1-3 and 15, Schneier discloses a method for transferring a key by encrypting the first electronic key using a first encryption key of the key provider; transferring the encrypted first electronic key from the key provider system to the second other system via the information network; and decrypting the encrypted first electronic key using the second encryption key stored within the first secure module and to store the decrypted first electronic key wherein the second encryption key is only for decrypting encrypted electronic keys (see section 8.3) and the key encrypting keys should be of greater length than the key it is encrypting (see page 177 and pages 166-167).

Schneier fails to disclose the three different types of keys (i.e. super root key, root key and private key); the encrypting and decrypting being performed in a secure module containing a processor and ROM; and the keys being un-modifiable and un-accessible outside of the module.

However, Ober et al teaches three different levels of keys (see column 3 lines 1-22 where the LSV is the super root key, the GKEK is the root key and the remaining keys are the private keys) Arnold teaches a secure module components (see column 3 lines 48-61) and Fischer teaches the properties of the keys (see column 4 line 56 through column 5 line 7).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use three levels of keys and Arnold's secure module with the properties of Fischer in the key transferring system of Schneier.

Motivation to do so would have been to provide a comprehensive powerful and secure encryption key management scheme (see Ober et al column 1 lines 49-51) to efficiently execute encryption algorithms (see Arnold column 3 lines 48-61) and to protect against contamination (see Fischer column 4 line 56 through column 5 line 7).

As per claims 4 and 16-18, the modified Schneier, Ober et al, Arnold and Fischer system discloses the processor internal to the module accesses the second encryption key only in response to a request from a corresponding secure module (as rejected above where it is implied that since the key is only used to encrypt other keys it wouldn't be used unless it is requested and as rejected in claims above).

As per claims 5-6, the modified Schneier, Ober et al, Arnold and Fischer system discloses using asymmetric and symmetric keys (see Arnold column 3 lines 48-61).

As per claims 7-8, the modified Schneier, Ober et al, Arnold and Fischer system discloses generating a first electronic key within a key-generating processor internal to the key provider system within a secure module (see Schneier section 8.3 in the secure module of Arnold).

As per claim 9, the modified Schneier, Ober et al, Arnold and Fischer system discloses the first electronic key is a root key for use in at least one of encrypting and decrypting private encryption keys (see Schneier section 8.3).

As per claims 28 and 30, the modified Schneier, Ober et al, Arnold and Fischer system discloses the bit length of the first super-root key is between about 2048 bits and about 4096 bits, the bit length of the first root key is between about 512 bits and about 2048 bits, and the bit length of any of said private keys is between about 128 bits and about 1024 bits (see Ober et al column 2 lines 47-60).

6. Claims 10-14 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold and Fischer system as applied to claims 1, 6 and 15 above, and further in view of Spelman et al (US 5680458).

As per claims 10, the modified Schneier, Ober et al, Arnold and Fischer system fails to disclose second and third encryption keys being stored.

However, Spelman et al teaches such keys (see column 2 lines 4-17 where the second and third keys are of the plurality of keys).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to store Spelman et al's keys in the modified Schneier, Ober et al, Arnold and Fischer system.

Motivation to do so would have been to have more than one root key (see Spelman et al column 2 lines 4-17).

As per claim 11, the modified Schneier, Ober et al, Arnold, Fischer and Spelman et al system discloses encrypting a fourth encryption key using one of the third encryption key and a key corresponding to the third encryption key; transferring the encrypted fourth encryption key from the key provider system to the second other system via the information network; providing the encrypted fourth encryption key to the processor internal to the first secure module of the second other system; and, executing program code on the processor internal to the first secure module to decrypt the encrypted fourth encryption key using the third encryption key stored within the memory circuit of the first secure module and to store the decrypted fourth encryption key within the memory circuit of the first secure module at a location corresponding approximately to the location where the second encryption key was stored (see Schneier and Arnold as applied to Spelman et al's key).

As per claim 12-13, the modified Schneier, Ober et al, Arnold, Fischer and Spelman et al system discloses replacing the second and third keys (see Spelman et al column 2 lines 4-17) and root key encrypting keys (see Spelman et al's keys as applied to Schneier and Arnold's key exchange system).

As per claim 14, the modified Schneier, Ober et al, Arnold, Fischer and Spelman et al system discloses erasing the second encryption key from a first storage area of the memory circuit; and, storing the decrypted fourth encryption key within approximately the same first storage area of the same memory circuit (see Spelman et al column 2 lines 4-17 where it is implied that a replaced key is erased).

As per claim 29 the modified Schneier, Ober et al, Arnold, Fischer, and Spelman et al system discloses the bit length of the first super-root key is between about 2048 bits and about 4096 bits, the bit length of the first root key is between about 512 bits and about 2048 bits, and the bit length of any of said private keys is between about 128 bits and about 1024 bits (see Ober et al column 2 lines 47-60).

7. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold and Fischer system as applied to claim 18 above, and further in view of Easter et al (US 559889).

As per claim 19 the modified Schneier, Ober et al, Arnold and Fischer system fails to disclose the module is FIPS 140 compliant.

However, Easter et al teaches such a compliant module (see column 6 lines 13-21).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to have the module of the modified Schneier, Ober et al, Arnold and Fischer system be FIPS 140 compliant.

Motivation to do so would have been to allow for top security (see Easter et al column 6 lines 13-21).

8. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold, Fischer and Easter et al system as applied to claim 19 above, and further in view of Bergum et al (US 5249277).

As per claim 20, the modified Schneier, Ober et al, Arnold, Fischer and Easter et al system fails to disclose a tamper detection circuit for erasing every cryptographic key stored within the memory circuit in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.

However, Bergum et al teaches such a method of tamper protection (see column 4 lines 7-32).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to apply this method of tamper protection to the modified Schneier, Ober et al, Arnold, Fischer and Easter et al system.

Motivation to do so would have been to provide maximum key security (see Bergum et al column 4 lines 7-32).

9. Claims 21-24 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al,

Arnold, Fischer and Spelman et al system as applied to claim 10 above, and further in view of Mason et al (US 6331784).

As per claims 21-24 the modified Schneier, Ober et al, Arnold, Fischer and Spelman et al system discloses the claimed limitations as in claim 10 above, but fails to disclose the keys only being erasable by the program code.

However, Mason et al teaches a system with an erase only mode (see column 2 lines 39-47).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate Mason et al's erase only mode in the modified Schneier, Ober et al, Arnold, Fischer and Spelman et al system.

Motivation to do so would have been so no information can be read from the device (see Mason et al column 2 lines 39-47).

10. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, and Mason et al system as applied to claim 24 above, and further in view of Ehrsam et al (US 4386234).

As per claim 25, the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, and Mason et al system fails to disclose the substantially non-volatile reprogrammable memory circuit is one of an electrically erasable read-only memory circuit and a random access memory circuit having an on-board power supply in the form of a battery. However, Ehrsam et al teaches such a memory having a battery (see column 13 lines 45-50).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Ehrsam et al's battery powered memory in the modified Schneier, Arnold, Fischer, Spelman et al, and Mason et al key exchange system.

Motivation to do so would have been to enable key retention when terminal power may not be present (see Ehrsam et al column 13 lines 45-50).

As per claim 31, the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, and Mason et al system discloses the bit length of the first super-root key is between about 2048 bits and about 4096 bits, the bit length of the first root key is between about 512 bits and about 2048 bits, and the bit length of any of said private keys is between about 128 bits and about 1024 bits (see Ober et al column 2 lines 47-60).

11. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, Mason et al, and Ehrsam et al system as applied to claim 25 above, and further in view of Easter et al (US 559889).

As per claim 26 the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, Mason et al, and Ehrsam et al system fails to disclose the module is FIPS 140 compliant.

However, Easter et al teaches such a compliant module (see column 6 lines 13-21). At the time of the invention it would have been obvious to a person of ordinary skill in the art to have the module of the modified Schneier, Arnold, Fischer, Spelman et al, Mason et al, and Ehrsam et al system be FIPS 140 compliant. Motivation to do so would have been to allow for top security (see Easter et al column 6 lines 13-21).

12. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, Mason et al, Ehrsam et al, and Easter system as applied to claim 26 above, and further in view of Bergum et al (US 5249277).

As per claim 27, the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, Mason et al, Ehrsam et al, and Easter system fails to disclose a tamper detection circuit for erasing every cryptographic key stored within the memory circuit in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion. However, Bergum et al teaches such a method of tamper protection (see column 4 lines 7-32).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to apply this method of tamper protection to the modified Schneier, Arnold, Spelman et al, Ehrsam et al, and Easter et al system.

Motivation to do so would have been to provide maximum key security (see Bergum et al column 4 lines 7-32).

Response to Arguments

13. Applicant's arguments filed 07/28/2006 have been fully considered but they are not persuasive. Applicant argues that the cited portions of Schneier do not correspond to the steps of claim 1; Schneier fails to disclose the secure module; the modified Schneier, Arnold and Fischer systems fails to disclose the "first root key" the "first super rot key" and the private encryption keys"; Ober fails to supplement the above deficiencies; Examiner used the claims as a frame to make the rejection; and the remaining references fail to make up for the above deficiencies.

With respect to Applicant's argument that the cited portions of Schneier do not correspond to the steps of claim 1, these portions of Schneier are relied upon to show a teaching of transferring a key by encrypting the first electronic key using a first encryption key of the key provider (key encrypting key);

transferring the encrypted first electronic key from the key provider system to the second other system via the information network (Alice sending Bob the encrypted key); and decrypting the encrypted first electronic key using the second encryption key stored within the first secure module and to store the decrypted first electronic key wherein the second encryption key is only for decrypting encrypted electronic keys (Bob obtaining the key by decrypting it with the key encrypting key for use in secure communications). These steps are the underlying method provided by the claims.

With respect to Applicant's argument that Schneier fails to disclose the secure module, Schneier disclose the key-encrypting key can be stored on a tamperproof device. Furthermore, the combined reference of Arnold teaches a secure module with the specified components (see column 3 lines 48-61).

With respect to Applicant's argument that the modified Schneier, Arnold and Fischer systems fails to disclose the "first root key" the "first super rot key" and the private encryption keys", these references were not relied upon to teach these limitations, Ober was relied upon to teach the "first root key" (the GKEK) the "first super rot key" (the LSV) and the "private encryption keys" (the remaining keys) (see Ober column 3 lines 1-22 and Figure 4).

With respect to Applicant's argument that Ober fails to supplement the above deficiencies as described above Ober teaches the "first root key" (the GKEK) the "first super rot key" (the LSV) and the "private encryption keys" (the remaining keys) (see Ober column 3 lines 1-22 and Figure 4).

With respect to Applicant's argument that Examiner used the claims as a frame to make the rejection it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). Therefore because each reference provides motivation as to why at the time of the invention one of ordinary skill in the art would make the proposed modification the rejections are proper. Also, with Applicant's use of the term "mosaic" Applicant appears to also be stating the Examiner has used too many references to render the claim non-obvious. However, reliance on a large number of references in a rejection does not, without more, weigh against the obviousness of the claimed invention. See *In re Gorman*, 933 F.2d 982, 18 USPQ2d 1885 (Fed. Cir. 1991).

Applicant's argument that the remaining references fail to make up for the above deficiencies is moot in view of the above response.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER